A Novel Approach for Detection of Routes with Misbehaving Nodes in MANETs

Sowmiya Hariharan[1], Jothi Precia[2], Suriyakala.C.D[3], Prayla Shyry [4]
(Sathyabama University, Department of Electronic Sciences, Chennai, India)
sowmiyahariharan@gmail.com
(Sathyabama University,Department of Telecommunication, Chennai, India)
preshiya@gmail.com
(Sathyabama University,Department of Electronic Sciences, Chennai, India)
cdsuriyakala@yahoo.com
(Sathyabama University,Department of Electronic Sciences Chennai,India)
suja200165@yahoo.com)

***Abstract*-Network nodes in MANET's are free to move randomly. Therefore, the network topology may change rapidly. Routing protocol for MANET's are used for delivery of data packets from source to the desired destination, Routing protocols are also designed based on the assumption that all the participating nodes are fully cooperative. However, due to the scarcely available battery based energy, node behaviours may exist. One such routing misbehaviours is that some nodes may be selfish by participating in route discovery and maintenance process, but refuse to forward the packet in order to save its energy. To solve this problem we propose a reputation based scheme where the watch dog uses a passive overhearing of nodes and assign a value to it as an appreciation or add nuggets to them. In this proposal, nodes with highest value are highly recommended for data forwarding and allow nodes to avoid the use of misbehaving nodes in future route selection. AdHoc On Demand Distance vector routing protocol may be used to get the recommendation details of the node intended to forward the packet from the neighbouring nodes. This paper proposes a novel method to mitigate the route with misbehaving nodes and also suggests a way to find if any intruder is present in the cluster of participating nodes using security aware AODV protocol.**

***Key Words*-Mobile AdHoc Networks(MANET's), Routing Misbehaviour, Selfish nodes, AdHoc On Demand Distance Vector Routing Protocol (AODV).**

I. INTRODUCTION

A. MANETs

Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers [1]. The operation of MANETs does not depend on pre existing infrastructure or base stations .Network nodes in MANETs are free to move randomly. Therefore, the network topology of a MANET may change rapidly and unpredictably. All network activities, such as discovering the topology and delivering data packets, have to be executed by the nodes themselves, either individually or collectively. The Structure may vary from small, static to a large, mobile network.There are two types of MANETs: closed and open [2]. In A closed MANET, all mobile nodes cooperate with each other toward a common goal. In an open MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity.

However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment[1]. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources.

B. Selfish or Misbehaving

An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behaviour is termed selfishness or misbehaviour. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy[3].

C. WatchDog and PathRater

The watchdog technique identifies the misbehaving nodes by overhearing on the wireless medium. The watchdog technique is based on passive overhearing. Unfortunately, it can only determine whether or not the next-hop node sends out the data packet. The pathrater technique allows nodes to avoid the use of the misbehaving nodes in any future route selections.

D. Security Attacks

The intruder attacks are minimized and removed by using Security Attack AODV. Which rechecks the presence of the node which sends the shortest path by getting the routing table details of the intermediate node present adjacent to the node with the shortest distance. Hence the intruder nodes are removed from the Infrastructure

We have done a detailed literature survey in this above mentioned work. Based on this we have studied that several techniques have been proposed / ongoing to detect and alleviate the effects of selfishness in MANET's. In Section 2, we deal with the various schemes used to prevent selfishness in MANETS, followed by section 3 which describes 2ACK scheme. In Section 4, we explain the Routing Misbehaviour Model followed by section 5 which deals with a cluster based evaluation scheme. Section 6 describes the novel proposal which we forward and also under research

DOI: 01.IJNS.02.01.151

work and last section concluded with expected result which we will achieve with better performance.

II. Existing Techniques

The security problem and the misbehaviour problem of wireless networks including MANETs have been studied by many researchers e.g. [1], [2], [3], [4].Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: *credit-based schemes* and *reputation-based schemes*. The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services.

They proposed two models: the Packet Purse Model and the Packet Trade Model. In the Packet Purse Model, Nuggets are loaded into the packet before it is sent. The sender puts a certain number of nuggets on the data packet to be sent. Each intermediate node earns nuggets in return for forwarding the packet. If the packet exhausts its nuggets before reaching its destination, then it is dropped. In the Packet Trade Model, each intermediate node "buys" the packet from the previous node for some nuggets and "sells" it to the next node for more nuggets. Thus, each intermediate node earns some nuggets for providing the forwarding service and the overall cost of sending the packet is borne by the destination [1].

The second category of techniques to combat node misbehaviour in MANETs is reputation-based [2], [6]. In such schemes, network nodes collectively detect and declare the misbehaviour of a suspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network.

The watchdog detection mechanism in [2] has a very low overhead. Unfortunately, the watchdog Technique suffers from several problems such as ambiguous collisions, receiver collisions, and limited transmission power. Noting that a misbehaving node can either be the sender or the receiver of the next-hop link, we focus on the problem of detecting misbehaving links instead of misbehaving nodes. In the next-hop link, a misbehaving sender or a misbehaving receiver has a similar adverse effect on the data packet [1].

III. Routing Misbehaviour

We focus on the following routing misbehavior: A selfish node does not perform the packet forwarding function for data packets unrelated to it. However, it operates normally in the Route Discovery and the Route Maintenance phases of the DSR protocol. The misbehaving nodes, however, refuse to forward the data packets from the source. The new Route Discovery phase will return a similar set of routes, including the misbehaving nodes. Eventually, the source node may conclude that routes are unavailable to deliver the data packets. As a result, the network fails to provide reliable communication for the source node even though such routes are available.

In guaranteed services such as TCP, the source node may either choose an alternate route from its route cache or initiate a new Route Discovery process.. Several routing and forwarding attacks on DSR are under consideration [5]. We concentrate in our work, mainly the protection No forwarding, Unusual attraction , Route salvaging,Lack of error messages,Unusually frequent route updates,Silent route change.

To overcome the adverse affect of using the DSR protocol, we propose an AdHoc On Demand Distance Vector Routing protocol. On Demand AODV, send the RouteRequest to all the intermediate nodes present in the network and the source in effect get the RouteReply with the path to be traversed by the data packets to reach the destination.This process reduces the overhead as it does not require to update the table periodically also there are few chances of old route or broken route being present in the routing table. The Route Request doesn't require to travel till the destination, any intermediate node having the details of the shortest path till destination will send a reply to the source sending the request.

The control overhead of misbehaving nodes and the delivery ratio of misbehaving nodes with comparison to AODV routing protocol and DSR routing protocol are graphed Refer Fig.2. and Fig.3. Using CONFIDANT Protocol the Reputation System modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an Alarm message sent out by the Trust Manager.

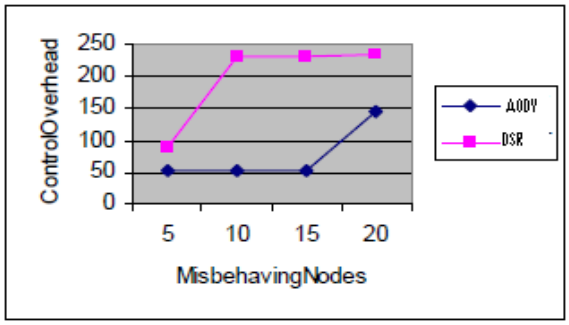

Fig.2. Control Overhead of Misbehaving Nodes

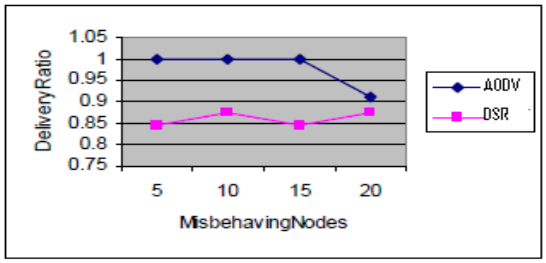

Fig.3. Delivery Ratio of Misbehaving Nodes

The lack of energy resources may cause a selfish node to drop legitimate packets which eventually disrupt the network performance. The victim of the misbehaved

DOI: 01.IJNS.02.01.151

node will become the reporter of this deviation act by sending a secret accusation to the central authority. The central authority is the centrepiece that processes the accusation and issue a trustworthy conviction to the misbehaved nodes,such penalization is deemed network-wide[3].

IV. PROPOSAL FOR DETECTION OF ROUTES WITH MISBEHAVING NODES IN MANETS

There are two scenarios to be dealt with. Firstly, we are mitigating the node which does selfish routing by misbehaving while forwarding the data packets and secondly, finding out if any intruder is present in the network having routes to reach the destination and removing the intruder attacks.

A. Mitigating the Misbehaving nodes

Routing protocol for MANET's are used for delivery of data packets form source to the desired destination, Routing protocols are also designed based on the assumption that all the participating nodes are fully cooperative. However, due to the scarcely available battery based energy, node behaviour may exist. To solve this problem we propose a reputation based scheme where the watch dog uses a passive overhearing of nodes and assign a value to it also uses Confidant protocol with four parameters- the Mmonitor, the Reputation based system, the Path Manager, the Trust Manager Respectively. In this proposal, nodes with highest value are highly recommended for data forwarding and allow nodes to avoid the use of misbehaving nodes in future route selection. An AdHoc On Demand Distance vector routing protocol is used to get the recommendation details of the node intended to forward the packet from the neighbouring nodes, which in turn preserves the battery of the node to forward the packet and remain in infrastructure for a longer time without misbehaving.

B. Avoiding Intruders

In infrastructure less network with mobile nodes, there are a number of well-known attacks. These include

• Denial of Service: A network service is not available due to overload or malfunction.
• Information theft: Information is read by an unauthorized instance.
• Intrusion: Access to some restricted service is gained by an unauthorized person.
• Tampering: Data is modified by an unauthorized person

The intrusion detection community has been focused primarily on wired networks. A relationship among the likelihood of detecting an intrusion and the amount of nodes that must take part in the process of detecting intrusions has been probed by them. Activities on the networks have been observed and compared with known attacks by signature-based IDS. On the other hand, new unidentified threats can be detected A Security Aware AdHoc On Demand Distance Vector Routing Protocol is used in order to check if no malicious nodes are present in the infrastructure that is used to reach the destination. The Intruder present in the cluster sends the source the shortest distance to the destination. The source with the routing table sends the request to the adjacent nodes present to the intermediate node which has the shortest distance. The neighbouring nodes check the route till destination and informs if they are correct. This security framework involves:Detection of malicious nodes by the destination node, Isolation of malicious nodes by discarding the Path.Thus, the malicious node having no route till the destination is found and removed from the infrastructure.

VII. CONCLUSION

In this paper we propose a new technique called recommendation based approach for detection of routes with misbehaving nodes in MANETs. The highlights of our new design will be as follows.(1)The misbehaving node is mitigated instead of the whole route since there may be only one route to reach the destination and in removing the route would have made the destination unreachable.(2) Identifies dishonest peers by constant evaluation on the node behaviour.(3) No false alarms can be raised by individual nodes.(4) AODV routing protocol reduces overhead and does not require to update tables frequently.(5) Security Aware AODV mitigates the malicious nodes.

REFERENCES

[1] Kejun Liu, Jing Deng, Member, IEEE, Pramod K. Varshney, Fellow, IEEE, and Kashyap Balakrishnan, Member, IEEE, "An Acknowledgment-Based Approach for the Detection of Routing Misbehaviour in MANETs", IEEE Transactions on mobile computing, Vol. 6, NO. 5, May 2007.

[2] Dhanalakshmi, Dr.M.Rajaram ," A Reliable and Secure Framework for Detection and Isolation of Malicious Nodes in MANET",IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.10, Oct2008

[3] Zan Kai Chong1, Moh Lim Sim1, Hong Tat Ewe2, and Su Wei Tan ," Separation of Detection Authorities (SDA) Approach for Misbehavior Detection in Wireless Ad Hoc Network",PIERS ONLINE, VOL. 4, NO. 8, 2008.

[4] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug. 2000.

[6] Z.Yan, P. Zhang and Teemupekka Virtanen, Trust evaluation Based Security Solution in Ad Hoc Networks, Technical Report, Nokia Research Center, Helsinki, Finland, Oct. 2003.

DOI: 01.IJNS.02.01.151